WRITTEN TESTIMONY OF FERNANDO BURBANO,

DEPARTMENT OF STATE CHIEF INFORMATION OFFICER

CHAIR, OPAP INTERAGENCY TECHNOLOGY SUBCOMMITTEE

CHAIR, CRITICAL INFRASTRUCTURE PROTECTION SUBCOMMITTEE

Presented to

THE HOUSE COMMITTEE ON INTERNATIONAL RELATIONS

JUNE 22, 2000

TABLE OF CONTENTS

LIST OF FIGURES

Introduction

The Department of State has undertaken vigorous activities that have resulted in significant achievements in three areas:

- Computer Security
- Compliance with the Overseas Presence Advisory Panel (OPAP) Report
- Capital planning and modernization

This report will address our initiatives and accomplishments in these areas.

COMPUTER SECURITY

The Department of State takes security matters very seriously. As examples of its commitment to Critical Infrastructure Protection (CIP), the State Department hosted the CIO Council Security Awareness Day, a CIP day and a Hacker briefing open to the entire Federal IT community. We also hosted a Cyber-threat Summit in November 1999, which featured world-renowned IT security experts and was moderated by CNN.

My focus over the last eighteen months has been threefold. First, measures have been instituted to improve our cyber security through enhanced business processes and technologies. Second, real-time tracking mechanisms to actively monitor our globally dispersed technology assets and infrastructure have been developed and deployed. Finally, we have instituted processes to continually assess the rigor and currency of our security improvement efforts through self-assessment activities including independent penetration tests, vulnerability assessments, and reviews of our controls and response mechanisms. We have successfully remediated findings of independent penetration tests conducted by the Lawrence-Livermore National Laboratory from June to August 1998, and Secure Computing in November 1999.

GAO Security Findings

COMPUTER SECURITY Pervasive, Serious Weaknesses Jeopardize State Department Operations, GAO/AIMD-98-145, May 1998, disclosed details of a GAO audit and recommended remedial measures. The GAO audit, which included an independent penetration test of our systems, identified 72 findings in six categories and eight management recommendations. Since my arrival at the Department of State we have addressed all of these items as previously addressed.

Assistant Secretaries of all appropriate business units have since reported 100% remediation and closure of these findings and recommendations. We have remediated our UNIX based systems by developing Configuration Management (CM) guidelines, reconfiguring the Network Management Stations and Workstations, and upgrading the firewalls. All configuration anomalies in a number of our Windows NT Servers and Workstations have been remediated through training and self-assessment tools (Kane Security Monitor). We have remediated our Dial-in Access capability by reconfiguring

modem connections and incorporating war dialing, which is now part of a program DS is performing on a regular basis. We have remediated our physical security, namely our handicap turnstiles, which have been upgraded to be fully compliant with both security requirements and the Americans with Disabilities Act. All routers have been brought into centralized management.

Summary of State Department Security Accomplishments

The Department of State accomplishments pertaining to IT security are summarized as follows:

**1.** Completed all actions recommended in the GAO security audit (GAO 98-145).
**2.** Achieved closure on FMFIA issues dating back to 1984.
**3.** Operated at full and uninterrupted capacity through Y2K.
**4.** Operated with minimal disruption through recent virus attacks.
**5.** Revised the Foreign Affairs Manual.
**6.** Drafted a System Security Program Plan based on guidance from GAO, OMB, and NIST, which is in review as we speak and is expected to be finalized no later than June, 2000.
**7.** Established and implemented an aggressive anti-virus program
**8.** Established continuous internal monitoring using an intrusion detection system.
**9.** Established and implemented a Computer Incident Response Capability (DoSCIRC) to respond to operational incidents, including a Computer Incident Response Team (CIRT) to respond to security incidents, including law enforcement issues. These teams are available around-the-clock.
**10.** Globally deployed a self-assessment COTS software tool, the Kane Security Analyst, under an enterprise license to all Information System Security Officers (ISSOs) and alternate ISSOs around the world. 400 copies of this are being deployed via DS. This deployment includes 233 foreign sites.
**11.** Established a continuous and rotating post and bureau evaluation program.
**12.** Initiated risk assessments of our classified, Sensitive but Unclassified, and Internet networks.
**13.** Initiated a joint effort with the NSA on a Public Key Infrastructure strategy to implement strong identification and authentication processes.
**14.** Initiated implementation of the risk management cycle as recommended in best practices published by GAO and OMB.
**15.** Inaugurated action to comply with the Chief Financial Officers Act of 1990 and the Paperwork Reduction Act of 1995 to ensure internal controls and security accountability for IT throughout the Department of State.
**16.** Initiated implementation of a robust certification and accreditation program incorporated within the recently released National Information Assurance Certification and Accreditation Process (NIACAP) embodied within the GAO recommendations.

Further details of the above items are disclosed in the following paragraphs.

GAO Security Findings

COMPUTER SECURITY Pervasive, Serious Weaknesses Jeopardize State Department Operations, GAO/AIMD-98-145, May 1998, disclosed details of a GAO audit and recommended remedial measures. The GAO audit, which included an independent penetration test of our systems, identified 72 findings in six categories and eight management recommendations. Since my arrival at the Department of State we have addressed all of these items as previously addressed.

Federal Managers Financial Integrity Act (FMFIA) issues

We have achieved closure of Federal Managers Financial Integrity Act (FMFIA) issues encompassing contingency plans, mainframe security, and information systems security. These issues are summarized as follows:

| | | | |
|---|---|---|---|
| Contingency Plans | Open | 1984 | Closed 1999 |
| Mainframe Security | Open | 1987 | Closed 1999 |
| Information Systems Security | Open | 1997 | Closed 2000 |

Y2K Rollover

The Department of State remained fully operational throughout the Y2K rollover. I directed the development of an ISSO Security Monitor (ISM) web site to handle cyber-based threats during the Y2K rollover. This web site is being revised to incorporate PKI, NIACAP, PDD-63, and Certification and Accreditation (C&A) links. We have successfully conducted and completed Sensitive But Unclassified (SBU) network penetration tests, a vulnerability assessment in agreement with PDD-63, and Y2K cyber penetration testing.

Responses to Cyber Attacks

The Department of State has also successfully repulsed numerous adversarial cyber attacks, including the May 2000 "Resume virus". Following NATO air strikes in Kosovo and Serbia, which included the accidental bombing of the Chinese Embassy in Belgrade, The Department of State encountered millions of e-mail assaults and approximately 250,000 hacking attempts. The Department of State maintained operations at full capacity. More recently, the "Love Bug" virus and variants thereof caused an estimated $10 Billion in damages globally. The Department of State did not experience any virus-inflicted data loss. Mission-critical operations were impacted only to the extent that any work-around activity, if needed, would have delayed the normal flow of business. From May 4, 2000 to May 8, 2000, a total of 99,570 hacking attempts were stopped at our firewalls.

The Foreign Affairs Manual (FAM)

We have updated the FAM Volumes 1 and 12 to reflect our security enhancements, modernization efforts, changes in roles and responsibilities, and compliance with GAO-recommended organizational structure

System Security Program Plan

We have also drafted an agency-wide System Security Program Plan, which will provide high-level guidance for program managers and users. This Systems Security Program Plan identifies and documents the diverse components comprising the Department's IT security program, identifies the functional bureaus responsible for development and implementation of the IT security program, and summarizes the guiding principles that serve as the foundation for IT security in the Department of State.

Establishment and Implementation of Key Controls

The Department of State has worked to establish and implement key controls which include an aggressive anti-virus program, continuous internal monitoring using an intrusion detection system, and around-the-clock availability of a two response teams. These are the Computer Emergency Response Capability (DoSCIRC) and the Diplomatic Security Computer Incident Response Team (CIRT).

The DoSCIRC responds to operational emergencies involving the Department of State Department computer systems by providing technical support and remediation. The DoSCIRC is centrally managed and has the ability to pull cross-functional experts who evaluate reported problems and devise appropriate response strategies.

The CIRT responds to computer security incidents on State Department networks. The CIRT is staffed by DS agents acting under authority of the Computer Fraud and Abuse Act of 1986, and is part of the Diplomatic Security/Analysis and Certification Division/Evaluation and Audit Branch (DS/ACD/EAB). The CIRT functions as a central reporting point that coordinates incident resolution with operational managers, outside computer security entities, and law enforcement entities as appropriate.

Improved Self-Assessment Capabilities

To improve our self-assessment capabilities, we have globally deployed the Kane Security Analyst (KSA) software tool under an enterprise license to strengthen the security posture of our offices. Kane Security Analyst (KSA) is a client/server security assessment tool that provides a fast, thorough analysis of client/server security for Windows NT and Novell NetWare. The KSA compares the client/server security

configuration with industry best practices or the local organizational security policy. In minutes, the client/server's areas of vulnerability can be discovered and corrective action taken. The KSA includes customizable reports that can be compiled into an attractive audit presentation for management. A global deployment of 400 copies of KSA has been initiated, including deployment and training to 233 foreign sites as well as domestic sites. This deployment is being carried out via the Diplomatic Security (DS) training office.

We have implemented a system to continually assess and evaluate our security policy and measures, which provides the capability to systematically improve our security posture. For example, we have established a continuous and rotating post and bureau evaluation program and are conducting risk assessments of our classified, Sensitive but Unclassified, and Internet networks, and we are working with the National Security Agency (NSA) on a Public Key Infrastructure strategy to implement strong identification and authentication processes. The roles and responsibilities of our post and bureau evaluation program are shown in Figure 1.

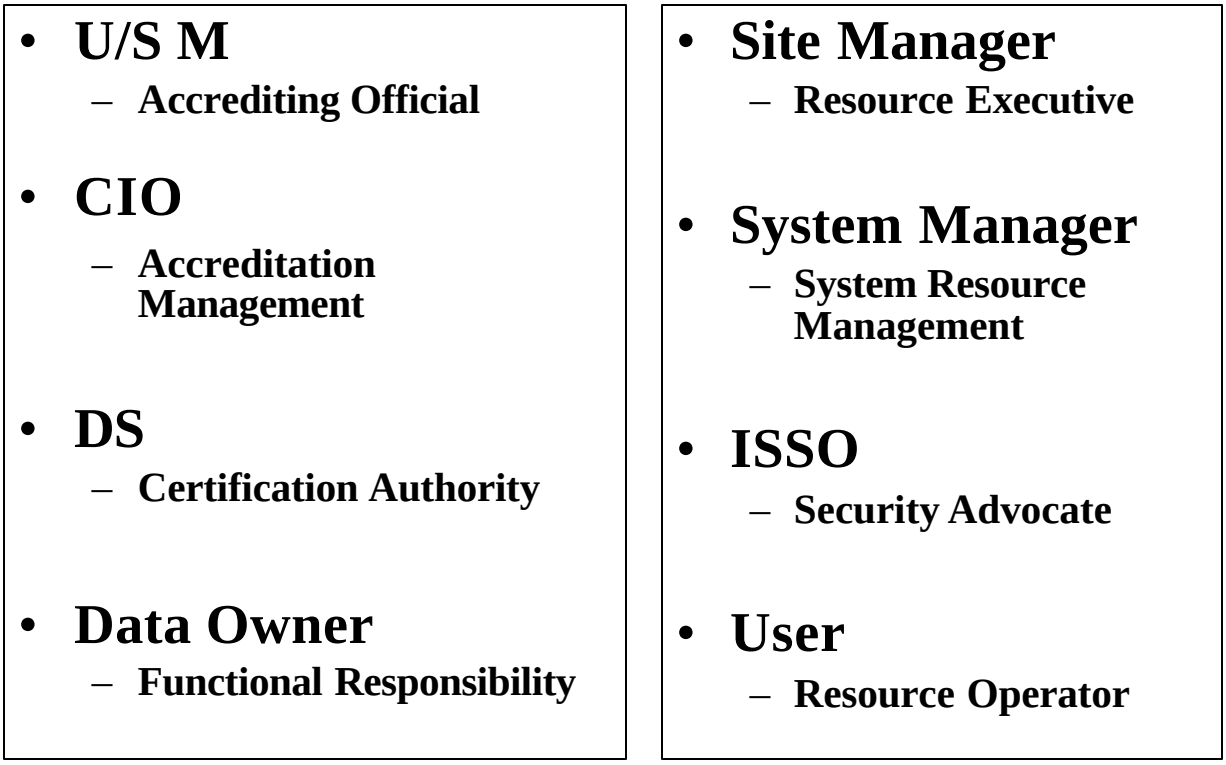


Figure 1. Computer Security Roles and Responsibilities

## Centralized Information Security

I established a Security Infrastructure Working Group (SIWG) to proactively oversee our enterprise infrastructure and coordinate an integrated department-wide security response. The SIWG is chaired by the Deputy CIO (DCIO) for Operations, and has representation from all Department Bureaus. The SIWG has achieved closure of the GAO Computer Security Audit by establishing a Tiger Team to remediate the findings and recommendations.

In December 1998, I established a centralized information security unit, the Corporate Information Systems Security Office, to oversee our enterprise infrastructure and coordinate an integrated department-wide security response. The CISSO, under the CIO, is responsible for managing and implementing the Department's computer security program. In this capacity the CISSO oversees accreditation management and infrastructure compliance functions within the Department.

## The National Information Assurance Certification and Accreditation Process (NIACAP)

I have also initiated involvement in the National Information Assurance Certification and Accreditation Process (NIACAP), which is defined by National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000. NIACAP establishes the minimum national standards for certifying and accrediting national security systems. NIACAP provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. NIACAP is designed to certify that the IT meets documented accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle. This model serves as a standard boilerplate for the development of a comprehensive certification and accreditation process.

The basic NIACAP certification and accreditation process model is shown as follows in Figure 2.

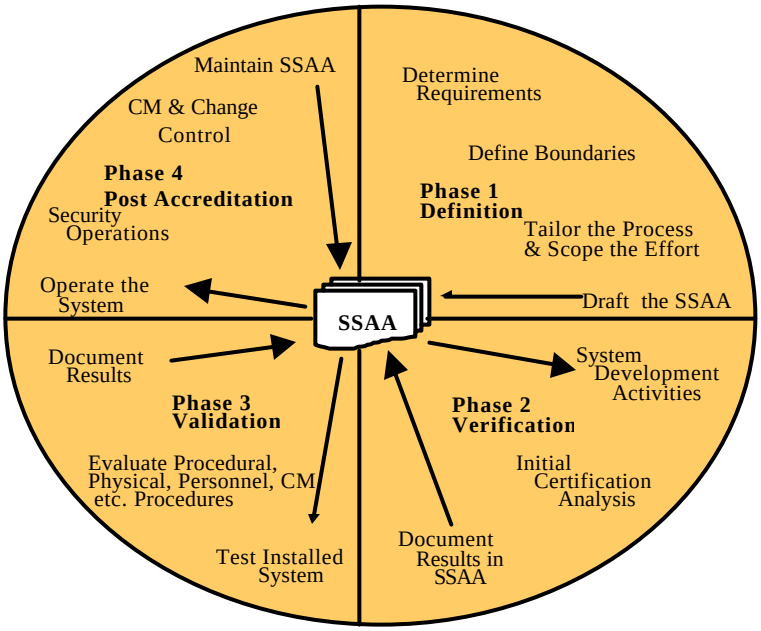


Figure 2. The NIACAP Certification and Accreditation Model

The Certification and Accreditation Program

The Department of State has initiated a strong Certification and Accreditation (C&A) program as recommended by GAO. The C&A program was established to ensure compliance with NIACAP requirements and specifically addresses the areas of policy, testing, and control. Within the context of the C&A program, certification and authentication are defined as follows.

- Certification - the comprehensive evaluation of technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

- Accreditation - Formal declaration by a Designated Approving Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable risk.

C&A involves four processes, the major components of which are summarized as follows:

1. Definition - Identify system roles, responsibilities, and security requirements; develop a C&A plan and determine level of effort; document negotiated items; incorporate existing documentation.

2. Verification - Analyze system architecture and software design; analyze network connection rule-compliance; analyze integrity of integrated products; analyze life

cycle management requirements; develop validation procedures, and conduct a vulnerability assessments.

3. Validation - Conduct a Security Test and Evaluation (ST&E); conduct penetration testing; verify TEMPEST compliance; validate COMSEC compliance; perform a system management analysis; conduct a site accreditation survey; perform a contingency plan evaluation; conduct a risk management review, document results.

4. Post-accreditation - Monitor physical, personnel, and management security practices for changes to security posture/profile; continue to verify TEMPEST and COMSEC compliance; maintain contingency plan; conduct risk-based management reviews.

Accreditation Management

The certification and accreditation process adopted by the Department of State consolidates the security mandates under the Computer Security Act, OMB A-130, and PDD-63 into a comprehensive life-cycle security process. This process simultaneously achieves the related goals of computer security and critical infrastructure protection. Through post-accreditation activities, including network monitoring and real-time configuration management tracking, the process continually verifies compliance with Department of State standards.

Throughout the process, close coordination with DS, OIG, and GAO, ensure that the key internal controls mandated by the Chief Financial Officers Act, Government Performance Results Act, and OMB A-11 are implemented in an effective manner. These controls ensure management responsibility and accountability for security and critical infrastructure protection requirements. As part of this process, vulnerabilities identified through the evaluations of auditing agencies will be incorporated into post-accreditation compliance activities to ensure that issues raised are resolved in a timely manner.

## OVERSEAS PRESENCE ADVISORY PANEL (OPAP)

### Introduction

To successfully advance our national interests, the foreign affairs community must be positioned to exploit the expansive access, speed, and analytical capabilities that information technology and rapid communications now afford. The leadership role of the United States in international affairs demands that we develop an integrated, responsive and secure IT capability, including systems and tools that enable us to access, manipulate, and share up-to-date information and to collaborate with others in addressing foreign policy issues. The Overseas Presence Advisory Panel (OPAP) report is the visionary blueprint for the future – one in which our interagency staff, wherever they are located, will have immediate access to the information, tools, and services needed for the conduct of e-Diplomacy in the Information Age.

The Department of State is heading the interagency effort to improve the information technology installed at our diplomatic missions around the world. As CIO for the Department, I had, in fact, already begun the planning to address many of the issues raised in the OPAP report. The Department of State's Information Technology Strategic Plan for first five years of the millennium describes five strategic IT goals as : 1) a secure global network and infrastructure; 2) ready access to international affairs applications and information; 3) integrated messaging; 4) leveraging IT to streamline operations; and, 5) sustaining a trained productive workforce. These five goals are consistent with the interagency OPAP IT goals. Thus, implementing the recommendations will build on work begun previously to meet agency specific goals.

Prior to issuance of the OPAP report, I had designated a Chief Knowledge Officer and initiated the creation of the Foreign Affairs System Integration Office (FASI) to plan for interagency connectivity. Under my direction, the Chief Knowledge Officer and Foreign Affairs Systems Integration Office are now dedicated to implementing the OPAP IT recommendations and are leading interagency groups in developing solutions.

The Department of State, in consultation with other Foreign Affairs agencies resident in our missions overseas, is planning for OPAP IT implementation at pilot posts in FY 2001. The pilot program will address the three IT-centered recommendations: 1) deploy an unclassified common, interoperable platform; 2) apply Internet and Internet-like technology to support interagency collaboration and streamline business processes; and, 3) provide a knowledge management system to share information between all Foreign Affairs agencies, wherever they are located.

### OPAP Report Recommendations

On February 10, the Department of State Under Secretary for Management, Bonnie Cohen, convened an interagency Overseas Presence Committee to address OPAP report concerns. Three interagency subcommittees have been established to deal with the

specific report recommendations concerning overseas facilities, interagency rightsizing of the total foreign affairs staff, and information technology. As CIO for the Department of State, I chair the OPAP Interagency Technology Subcommittee and membership includes the CIOs of the principal foreign affair agencies (recommendation 5.2). Two interagency IT working groups were also put in place: one for implementing Knowledge Management systems and the second to design the IT infrastructure and platforms ( Figure 3, graphically depicts the organizational structure of the various committees.)

To date, the cooperation between all of the foreign affairs agencies in developing solutions to the OPAP report recommendations has been outstanding. Through the CIO council and its various subcommittees, the CIOs have established strong relationships and have worked collaboratively on issues of common concern. The same spirit of cooperation has been brought to the OPAP Interagency Technology Subcommittee and associated working groups.

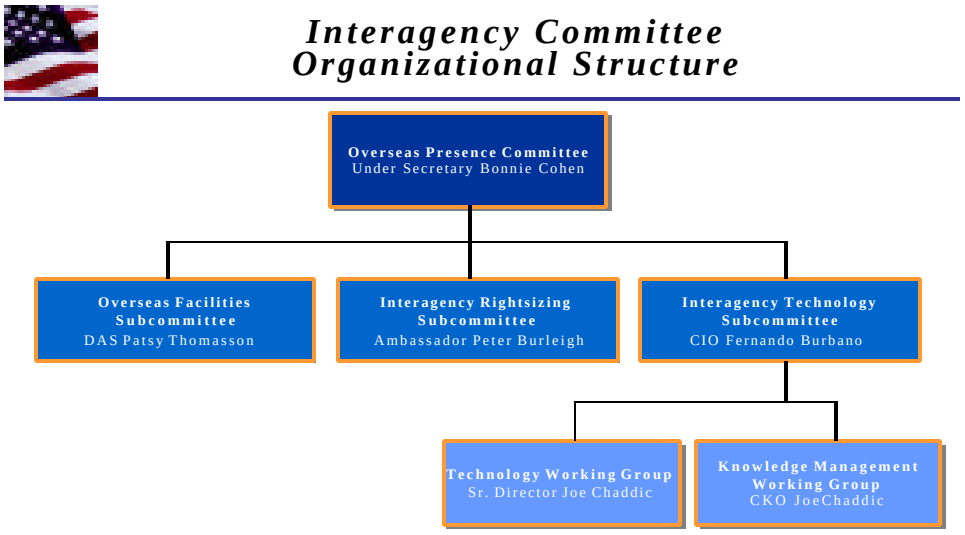


Figure 3. Interagency Committee Organizational Structure

The OPAP Interagency Technology Subcommittee will define: 1) a concept for an interagency, interoperable IT infrastructure; 2) a project plan to include development and testing of a prototype, along with field testing of the concept at two or more pilot posts as funding allows; 3) a cost model, which will be used to develop estimates for the two pilots; 4) a requirements survey; 5) preliminary design, architecture, standards and security proposals; and 6) a concept and design for a Knowledge Management system.

The upgraded information technology will improve interagency knowledge sharing and communications to enable regionalization and collaboration. Thus, the work of the Interagency Technology Subcommittee is being driven by requirements defined by the Rightsizing and Knowledge Management initiatives. The IT subcommittee has been

meeting regularly to collaborate, research, analyze, plan, and design the IT infrastructure and systems to comply with technology centered recommendations.

Six posts were identified as possible pilot sites for the OPAP rightsizing initiatives: Mexico City, Mexico, Paris, France, Tbilisi, Georgia, Amman, Jordan, New Delhi, India and Bangkok, Thailand. The chairman of the Interagency Technology working group accompanied members of the Rightsizing Subcommittee as they visited and evaluated the six posts. Based on trip findings, Mexico and India are recommended as primary candidates to pilot and test the OPAP IT solutions, conditional on the availability of timely and adequate funding.

The initial focus will be on the unclassified environment to support interagency connectivity for e-mail, safe Internet-like services to all foreign affairs agencies. Once the unclassified platform is tested, validated and fully deployed, we will progress to the classified platform, using the unclassified design as a model. We plan to utilize COTS products and existing agency platforms to the extent possible.

We have made significant progress in developing the concepts and frameworks for both the technology infrastructure and the knowledge sharing system. Specific recommendations of the intragency group regarding the infrastructure and knowledge management framework are being finalized. Thus information below is preliminary and relates to our approach for use of FY 2001 funding request by the Department for OPAP IT initiatives. The following provides a high level overview of the proposals to address the IT recommendations For the purposes of the pilot project:

OPAP IT Infrastructure - Conceptual Framework

Overview and Methodology

The OPAP Interagency Technical Study Group is studying an initial approach to implement a pilot infrastructure needed to enable all agencies, regardless of their location, to exchange e-mail and have an interoperable platform for knowledge sharing. A standardized project management approach is being be used to mitigate risk and to achieve IT recommendations presented in the Nov 1999 America's Overseas Presence in the 21st Century OPAP Report. Key items in our management approach to the project are:

- Establishment of formal Memoranda of Understanding between agencies;
- Consideration of Service Level Agreements;
- Formation of Interagency Governance Boards;
- Identification of Control Gates and interagency reviews;
- Tracking project milestones with appropriate reporting procedures including monthly status reports;

Implementation of a pilot program to test and validate the concept of operations and various technical alternatives;

- Evaluation of the pilot program and refinement of designs as necessary before proceeding with further deployment overseas;

OPAP IT High Level Architectural Concept

The Department of State has had some success with IT architectures, although we have more work to do. Our A Logical Modernization Approach (ALMA) platform, which represents an operational overseas, unclassified architecture, has been extremely successful. In addition, we have developed a high level IT Architecture (ITA) document to begin the process of establishing an architectural framework and a set of evolving standards to guide IT projects. In addition, we implemented a Configuration Control Board (CCB) and developed a high level IT Architecture (ITA) document to begin the process of establishing an architectural framework and a set of evolving standards to guide IT projects. The end result of these efforts is a remarkable level of consistency throughout the Department and around the world in terms of IT environment, especially for unclassified processing. This has resulted in increased ease of use for end users and technical support staff, and is enabling us to move forward with a global enterprise management initiative. We are now beginning to develop a parallel classified architecture.

We have been applying our architectural experience to the OPAP work, and have developed the high level pilot architecture presented below. Some key architectural principles we are planning to pursue are simplicity, flexibility, standards, and security. These principles greatly increase the chance of success, while reducing costs and risks. The high level OPAP architecture we have developed so far conforms to these principles. Key elements are that agencies need not change their architectures to connect to and use the OPAP facilities, and a range of connection options will be accommodated. Agencies need not install any special software, as a standard Web browser will be the primary common interface to the OPAP Collaboration Zone. We are modeling the pilot architecture on the Internet, where people can communicate from virtually any type of desktop or network connection. Internet like practices and tools that have so well enabled businesses and individuals to collaborate will be our model. We will refine this architecture as requirements and technical solutions become better understood.

Based on an initial set of requirements derived from the OPAP final report and information collected from the Foreign Affairs agencies, the proposed high level concept will allow all agencies access to an unclassified "network" through their existing LANs. The pilot concept proposes to create a number of "collaboration zones", which might be compared to AOL with robust security features to minimize vulnerabilities and risk of intrusion. The collaborative zone is the Foreign Affairs Community's network to share information and communicate via e-mail. The servers located in the Collaboration Zone would provide access to shared Knowledge Management data. Just like the Yahoo portal on the Internet, the collaborative zone allows users to search and interact with shared databases and applications belonging to any agency and located at any site.

The OPAP concept for interagency e-mail would provide quicker and more reliable delivery of messages and attachments than exists today. One approach to overcome the difficulties of interfacing with the current stovepipe systems is to provide robust e-mail service through a collaboration zones. This type of service would resemble an Internet

Hotmail account, making e-mail accessible from any location, using existing LANs and PCs.

By using Internet technologies, the Internet Browser at the desktop can be used to access the network and thus becomes the common platform called for in the OPAP IT recommendations. Agencies can continue to use their existing LANS, regardless of the operating system (MS NT, Banyan Vines, Apple, Novell, etc.); users will have access to the shared network with their desktop browser. Thus we do not expect agencies will have to make changes to their existing architecture. Our proposed pilot solution should be cost effective and achievable to comply with the OPAP recommendation of a common platform. We hope that in most cases agencies will not need to replace existing equipment.

To ensure a secure environment, the pilot architecture would include security-enabling technology, such as Public Key Infrastructure (PKI) for user authentication, data encryption, and firewalls at access points. The Department of State's Bureau of Diplomatic Security and the IRM Office of System Integrity will coordinate with other agencies' security elements to develop appropriate security requirements. A risk analysis and assessment will be conducted after a prototype test and prior to the pilot program deployment.

A depiction of the high level architectural concept for a pilot project is presented below in Figure 4, emphasizing the flexibility of connectivity options and the range of services to be provided by the proposed collaboration zone. The "behind the scenes" systems and security engineering that will be required to sustain the new IT environment is not represented in the diagram, but will be part of the more detailed system concept documents.

Conceptual Collaboration Zone Architecture

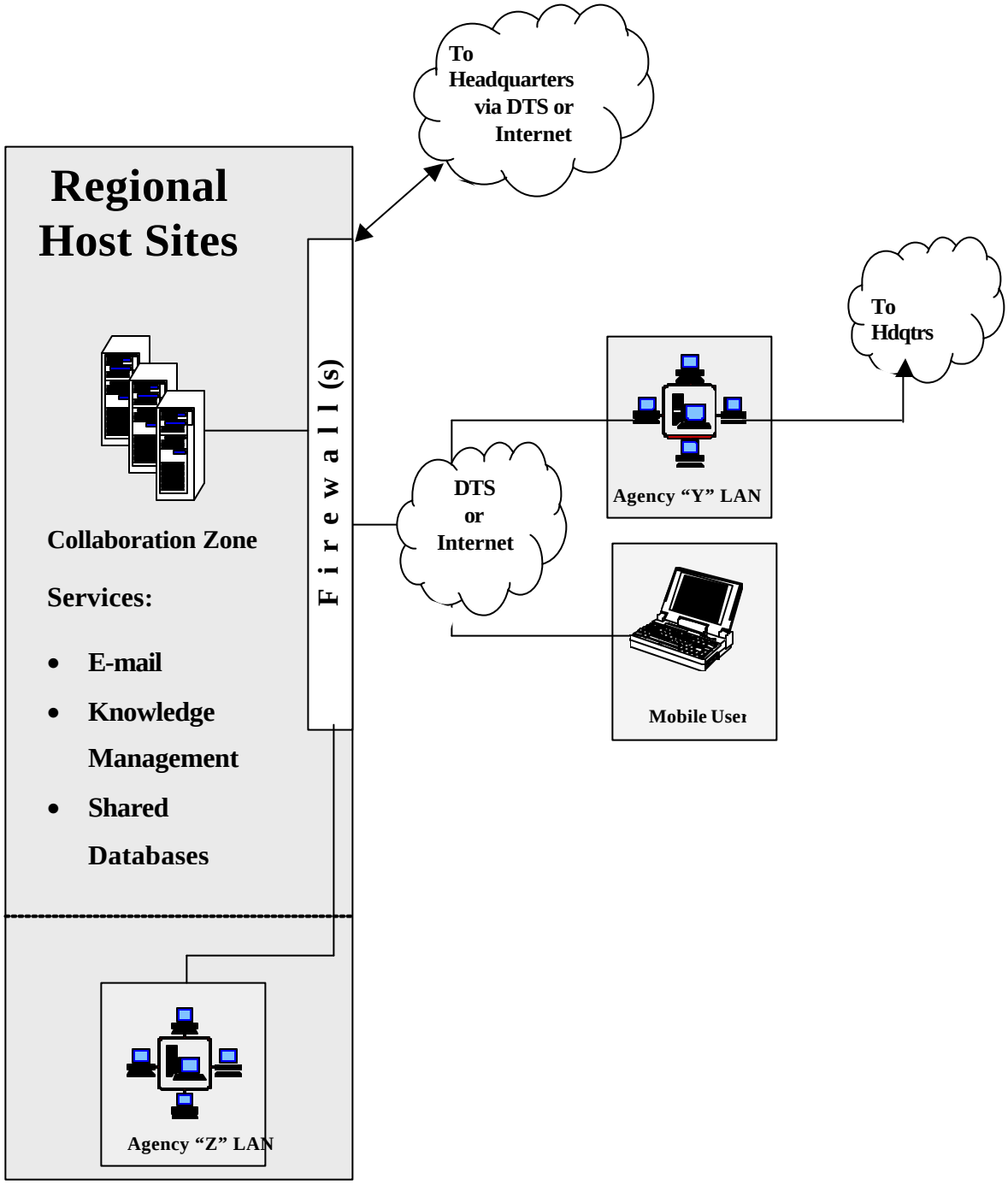


Figure 4. Conceptual Collaboration Zone Architecture

OPAP IT Infrastructure - High Level Requirements

Based on interagency discussions pertaining to Knowledge Management requirements and the common platform and Information Technology infrastructure to support knowledge sharing, the following is a synopsis of the high level requirements identified by the interagency working groups:

Knowledge Management Requirements:

Unclassified E-mail

Issue specific databases

Skills and Expertise Database

Workflow Applications

Discussion Groups Among Communities of Interest

Shared Applications

Information Repository for document sharing and collaboration

IT Infrastructure Requirements
Improve overall cost and quality of IT across the foreign affairs community

All agencies, wherever located, must be able to access the Collaboration Zone

Agencies can access the Collaboration Zone using Diplomatic Telecommunications Service – Program Office (DTS-PO) as a transport mechanism. Also able to access via Internet, dial-up, or other viable option.

Agencies cannot lose current functionality

Desktop system should be able to run TCP/IP stack and have a PKI capable web browser

Easily maintainable
- Low maintenance (minimum support staff needs)
- Remote management
- Low cost to implement

High availability
- Acceptable application performance
- Bandwidth available to meet needs

Applications must be web enabled on the front-end and PKI capable

Message Integrity

Data Confidentiality

Non-repudiation and Authentication

Security Hardware/Software Needs

Scaleable and extensible to include future expansion of Internet services where appropriate.

IT Infrastructure - Assumptions

Design for Sensitive But Unclassified[1] while allowing for unclassified.

Data owners to control access as needed.

Two possibilities exist for e-mail. These include: using existing agency e-mail systems and adding e-mail services to the collaboration zone.

Take advantage of existing Web Enabled applications.

Each agency must be able to establish connection to transport mechanism.

Connection standards will be developed.

Users will not have to be physically located at the post site.

OPAP Pilot Infrastructure - Open Issues

Availability of timely and sufficient funding for pilot posts.

Establishing and maintaining an organization process to manage the development, implementation and ongoing support of the collaboration system solution.

Clear policies and guidance on data security.

[1] Describes information which warrants a degree of protection and administration control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act.

Service levels for network, systems and applications.

Strategy for domain names and IP addressing.

Policies for providing remote access.

Current applications may not be web and PKI enabled.

Agreement on the PKI certificate process.

PKI technology is still in the pilot phase.

Configuration management.

Agency headquarters access and integration.

Integration with emergency action plans.

Agreement on Internet access policy.

OPAP Pilot Infrastructure Project - Minimizing, Avoiding, and Managing Risk

We are very comfortable dealing with the risks of large-scale overseas IT projects. We successfully deployed the ALMA IT infrastructure, Y2K modernization and remediation, and the overseas wireless modernization. We successfully addressed the numerous risks inherent in such an effort.

Some of the risks associated with OPAP are common to any IT project -- for example, delivering solutions on time and within budget. The Department of State has in place several processes for managing these types of risks. However, this effort also creates unique risks, due primarily to the interagency nature of the effort and the unclear functional scope. Unlike most IT projects, the potential scope is extraordinarily broad, and we must take aggressive steps to manage the scope, so we can deliver successfully.

We have taken several steps to address the major risks. General risk mitigation steps we have taken are:

1. We are developing a risk mitigation plan, identifying all known risks and establishing a disciplined process for monitoring these and other risks that may arise, and for addressing these risks to mitigate their impact.

2. We have limited the scope of initial efforts to unclassified systems, greatly reducing the security complications.

3. We are emphasizing commercial-off-the-shelf (COTS) solutions, reducing the need to develop high risk custom software.

4. We are proceeding incrementally, beginning with a prototype, then pilot implementation in two countries.. We will test and refine along the way, ensuring that risks are identified and resolved.

5. We will apply the disciplined IT project management process that The Department of State has been using successfully for all internal projects. This process, called Managing State Projects (MSP), will ensure that all phases of the OPAP effort go through appropriate control gates and decision points, and enabling management and the Interagency working groups to monitor progress and ensure success.

We need the support of Congress to help us address some of the most important risks. The schedule we are operating under is very aggressive, and we are currently developing a comprehensive project plan with milestones. In the course of developing this plan, it has become clear that one key variable affecting project success is timely availability of funds. There is virtually no slack in the schedule and, in fact, many tasks must be performed in parallel to achieve the deadlines. Accordingly, we can tolerate no delay in funding. We must be able to initiate procurements for the prototype as early in October as possible, and must have the funds to do so.

OPAP Project Timeline and Major Milestones

A standardized project management methodology is being employed. The project is currently in the "Study Phase." This phase will consider all viable deployment alternatives, select options based on a cost benefit analysis, develop and test prototype(s), and ultimately deploy pilot sites by September, 2001.

Milestone dates are dependent on adequate and timely availability of funding

**Project Milestones**

| | |
|---|---|
| Conceptual Framework | May-00 |
| **Initial Project Plan** | May-00 |
| Requirements Document | Jun-00 |
| Organizational Process Architecture | Jun-00 |
| **Preliminary Security Requirements** | Jun-00 |
| **Cost Benefit Analysis** | Jul-00 |
| Concept of Operations | Jul-00 |
| **Formal Project Plan** | Aug-00 |
| System Acquisition Plan for Prototype | Sep-00 |
| Prototype Implementation Plan | Oct-00 |
| System Integration Plan -- Prototype | Dec-00 |
| **Complete Prototype Testing** | Apr-01 |
| Formal Security Risk Analysis | Apr-01 |
| Revised Concept of Operations/ Project Plan | Apr-01 |
| System Acquisition Plan for the Pilots | Apr-01 |
| System Integration Plan -- Pilots | May-01 |
| Site Training Plan | May-01 |
| Pilot Post Deployment Plan | Jul-01 |
| **Complete KM Prototype Testing** | Sep-01 |
| **Deployment of IT Pilots Completed** | Sep-01 |
| **Deployment of KM Pilots Completed** | Dec-01 |

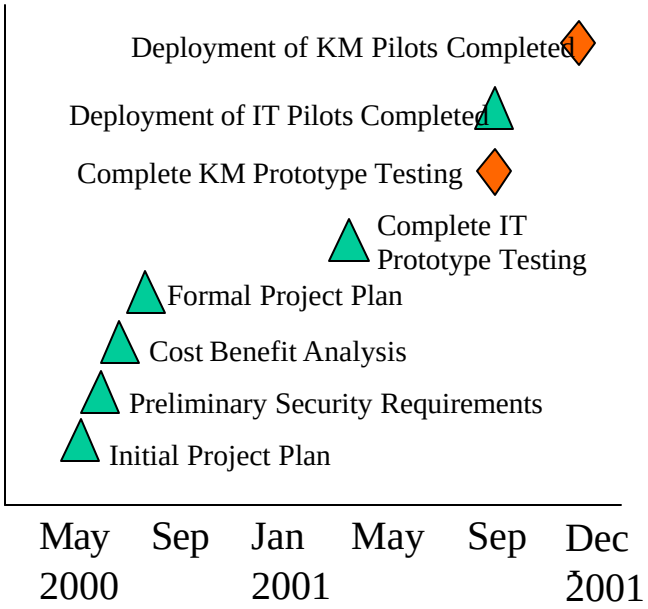


Figure 5. OPAP Major Milestones and Timeline

OPAP Knowledge Management – Conceptual Framework

Knowledge Management - Operational Concept

On April 4, the OPAP Knowledge Management Working Group published Initial Findings, including a prioritized listing of business functions at post which could accrue benefits from application of knowledge management tools and methods. Knowledge management tools are important components in the successful movement of post operations to a more collaborative, streamlined approach in line with the OPAP recommendations. The following is a high-level operational concept of the way that knowledge systems could support employees at the prototype and two pilot posts.

Knowledge Management - Scope

Organizations: The organizational scope for the knowledge management prototype and pilot projects will be the agencies participating in the right-sizing portion of the foreign affairs response to the OPAP Report. This includes the Departments of State, Defense, Commerce, Agriculture, Treasure, Justice, Transportation, the Peace Corps, the U.S. Agency for International Development, and other independent agencies.

Knowledge Systems Users: Participants in the Knowledge Management Prototype and Pilot Projects will be professionals representing their agencies at overseas posts or in Washington. At posts, the participants will be those employees who are working toward achievement of some aspect of the Mission Program Plan (MPP). It should be noted that the participating agencies vary widely in the statutory requirements and policies governing their overseas presence. Accordingly, each organization (and, hence, the users of knowledge systems) will approach joint knowledge systems differently. The material in this report represents a first draft of composite requirements across all participating agencies, not to suggest that all agencies at post would necessarily use all of the described functions. Future definition of detailed requirements will address these agency differences explicitly and will incorporate them at that time.

Classification Level: All requirements presented herein apply to Sensitive But Unclassified (SBU) information and SBU information systems.

OPAP Knowledge Management - Operational Concept

The Knowledge Management Prototype/Pilot Systems will seek to provide appropriate staff at post the following capabilities and functions:

1. Access to timely, reliable email service between agencies.
Employees will have the ability to send and receive unclassified email, including attachments, reliably and within a reasonable period of time. The first priority is to achieve this level of service between all organizations at post (includes organizations associated with the Embassy in country). In addition, that capability should extend outside the post environment, to the region and worldwide. Remote access capability (the ability to send and receive email, securely, from remote locations) is also highly desirable.

2. Access to news and information of interest to the post and the wider community.
Current news is the lifeblood of American overseas presence. The availability of late-breaking news on local and world issues allows employees at post to respond to events occurring in the host country and region as well as world issues. Equally important is access across the post community of news specific to the post.

a. Calendars: A calendar of events of general interest to the post will be available. Schedules of senior officials will be available for coordination, on a more limited basis.

b. Post/agency notices and announcements: Announcements and notices affecting the entire post will be available. Employees will be able to tailor the knowledge system to present notices from other selected organizations of interest.

c. Telephone directory: A post telephone directory will be available, and updateable by the individual. Department/Agency worldwide directories will be available in cases where such an on-line directory exists.

d. News services: All employees will have access to current local and world news and weather reports, with immediacy that is equivalent to availability of CNN. The news capability of the knowledge system will be tailorable by the employee to present the news of greatest interest either passively (with headlines on the "front page") or via "push" capability (the employee receives a tone or some other indicator that there are new headlines in their area of interest).

3. Ability to collaborate electronically across agencies on a wide range of issues.
The ability for professionals to collaborate electronically to achieve post objectives supports key aspects of the OPAP recommendations. This ability would allow workers to make the best use of their limited time and resources, and facilitates the participation of specialists regardless of geographic location. In addition, electronic collaboration improves the documentation of group activities, speeding up the learning process for those who are working on similar activities or joining the collaborative activity after it is underway. Knowledge system collaboration would allow teams of any level of formality or duration to develop "team rooms" wherein team plans, products and discussions can be developed and stored for future reference. The virtual nature of this capability allows teams to be comprised of any set of employees, located anywhere in the world. The following are examples of some areas in which this type of collaboration would be beneficial:

a. Crisis coordination: The knowledge system will support the rapid coordination needs of crisis situations, by providing the virtual "space" for crisis teams to compile plans and products and hold discussions. Crisis teams will be able to pull in expertise from other locations, as needed.

b. Support for Mission Performance Plan (MPP) "clusters": Agency representatives who are participating on issue teams aligned with the MPP will be able to meet and share products with other team members within virtual team "space". This capability will also allow the team to create repositories of information about cluster group activities for access and use by the wider community.

c. On-the-fly development of "space" for teams to use for coordination on a wide array of issues: Project or issues groups of any size will be able to create tailored "space" to meet their needs for discussion, development of products and repositories, research and consultation. Depending upon the level of technical support available at post, this process could be performed independently by team members, or by support staff located at the post or regionally.

4. Access to knowledge databases and repositories, both agency and community-owned.
current information systems environment does not support access to Department

databases and repositories by other Departments or Agencies. The knowledge systems will be designed so that Departments and Agencies may make available relevant databases and repositories of interest at post to a wider audience. The owner of each database/repository of information will define criteria for access to their information.

a. Existing databases and repositories: Each participating organization currently owns electronic research sources that could be of broader interest at post. The employee will be able to use these sources for research in cases where there is legitimate need and agreement by the owner of the resource that it is shareable. The originating organization must be able to specify the appropriate target audience for the information, and protections must be in place to assure that sharing the resource does not put the resource in jeopardy.

b. Sources developed as a result of collaboration: Products of working groups will be available to others working within the area of interest for research purposes. Team members will be able to identify work that was done on similar projects and issues within the post, the region or worldwide. This encourages use of lessons learned and development and use of best practices across the community.

c. Skills and expertise: Employees will be able to identify those within the foreign affairs community who have specific skills and expertise for purposes of consultation. Knowledge systems will be capable of capturing areas of skill and expertise based upon direct input as well as product publication and participation on virtual teams. This information will be available worldwide, allowing consultations to take place with sources of expertise quickly and with minimal cost.

d. Country or region-specific: All employees will be able to quickly and easily access information about products and issues organized by country and region. This capability will be particularly useful for orientation of employees recently arriving at post.

e. ICASS: Information about ICASS products and services as well as information currently contained within ICASS applications will be available for research. This capability will improve the ability of participating organizations to manage their ICASS activities.

5. Ability to use workflow applications to increase efficiency.

Workflow applications are computer programs which capture work transactions as they occur, streamlining the work process while organizing the captured information in ways that allow analysis, processing and distribution of the work being conducted. The result is reduced time to complete work processes, fewer instances of lost or mishandled transactions and greater efficiency of workflow. In addition, work processes accomplished this way are more easily quantified and analyzed, supporting trend analysis and decision-making. Employees will be able to "self-service" more often for both routine transactions and resource-related activities. The following are some examples of the areas where a workflow approach could be used to advantage:

a. Personnel: Offices at post will be able to process position classification requests, develop position descriptions, develop and manage performance plans and handle a wide array of personnel-related items electronically. It is important to note that the electronic nature of the transactions reduce the importance of the physical location of the specialists needed to complete the activities – work flows to the people who must work on the transaction no matter where they are located..

b. ICASS: ICASS service requests and a variety of other ICASS transactions will be available electronically, allowing representatives of each participating agency to know the status of ICASS work immediately.

c. Other administrative: Other areas suggested for workflow process include travel planning and management, training requests and feedback, financial and budget activities, procurement processes.

d. Contact management: Employees will have access to information about host country contacts, relationship history and links. Participants will be able to schedule meetings, conferences and other events, document contacts and add to the knowledge store. Options will be available to create mailing and distribution lists, and perform other work functions organizing contacts within the host country.

e. Motorpool scheduling: Post personnel will be able to interact with the motorpool office to schedule service.

f. Re-allocation of physical resources: Posts will be able to manage their excess property virtually, advertising availability of excess resources between agencies.

OPAP Knowledge Management - Summary of Architectural Requirements

The concept of operations outlined above infers a number of characteristics for the information technology architecture hosting the knowledge systems. Listed below are those characteristics. While the characteristics appear challenging when considering the current environment, they are necessary to support a robust interagency knowledge management environment.

**1.** The handling of email traffic must be changed to a method that allows more direct routing of email within the post and region. While some participating agencies have implemented methods to improve email flow between their personnel and the post (principally through using Internet email), this is not true across the board. In addition, several participating agencies noted the growing need for email access from remote locations (from example, from residences or while traveling).

**2.** Collaborative tools must be in place to support the functions outlined above. Discussions must be possible both asynchronously (meaning all parties do not need to be on-line at the same time) and synchronously (similar to the "chat" capabilities of

commercial on-line services, but using both voice and text). Capability must exist for group development of products and creation of data stores of a variety of types. It must be possible for groups to quickly develop team "space", either independently or with the support of a technical specialist at post or within the region.

**3.** The capability must exist to link to Department/Agency information sources that do not exist within the knowledge system. These information sources exist within the systems environments of the authoring Department/Agency. There must be capability to control access to the information per the requirements of the authoring organization, and in keeping with SBU security guidelines and practices. In all cases, access to this information is the prerogative of the authoring organization, and access rules are defined by that organization. Availability of this link must not jeopardize the information source.

**4.** The capability must exist to archive and manage the products and information holdings of the knowledge system(s). For example, collaborative activities, including discussions, plans, products and data stores should all be captured in a method which supports eventual archiving of the material.

**5.** The technical architecture must be able to support development and use of applications common to the participating agencies (to support workflow applications). The capability must exist to transfer work products between locations for workflow purposes.

**6.** Timely access to public news services must be available.

**7.** A key factor in design of architecture to meet these requirements is the low level of systems support resources available within most agencies at post. Remote administration should be considered, and to the extent that local administration can be simplified to not require involvement of systems professionals, this approach should be taken.

**8.** Participating agencies do not have financial resources to replace network operating systems or add substantial investments in hardware and software to their inventories. To the extent possible, information technology solutions should allow interface between the existing network and systems resources of participating agencies and the target architecture. Agencies should be able to exercise the option of fully integrating this solution into their existing networks or maintaining the knowledge systems as a stand-alone capability.

**9.** One candidate technology that holds promise to serve as a desktop interface to the listed capabilities is "portal" technology. One aspect of portals that make them particularly attractive for this application is the ability to tailor portals to the specific functional requirements of each worker, assuring that the information that they most need to see is presented quickly and in a manner that best suits the needs of the user.

**10.** Many of the listed requirements infer a method of populating the knowledge systems which is known as monitored self-posting. For most functions, professionals should be able to add information to the system, viewable by others, without requiring the assistance of a technical specialist. Monitoring capability should be available to allow oversight of the information being posted and editing of that information by an oversight organization. Particularly in the early stages of this program, it is important that there be a single point of accountability for the knowledge systems within the post, and that this entity be given responsibility for monitoring the content of the knowledge systems. It is important to provide guidance to first-time knowledge system participants regarding what is and is not appropriate content.

**11.** Operation of knowledge systems meeting the criteria contained herein will require telecommunications bandwidth beyond the level currently available to a large percentage of overseas posts. Bandwidth issues must be considered in the selection of knowledge tools and must be a key consideration in the development of the underlying technical architecture.

Knowledge Management - Personnel-Related Issues

**1.** FSN Classification
Full implementation of the described knowledge capabilities will change the day-to-day responsibilities of many personnel at post. Several participating agencies employ Foreign Service Nationals (FSNs) in key positions requiring contribution to and interaction with the knowledge systems. This has at least two implications requiring further action. First, it is recommended that, as this program proceeds, classification standards for FSN positions be reconsidered in light of the increased sophistication of the knowledge work required in their positions. In addition, the Working Groups must analyze the impact of this situation on security requirements for a Sensitive But Unclassified systems environment.

**2.** Training
Successful implementation of knowledge systems will require significant investments in training. Of particular importance is orientation of personnel to new expectations regarding the way they work and the way they think about the use and management of information sources.

Knowledge Management - Next Steps

In preparation for development of prototype and pilot knowledge systems, several near-term steps are required:

**1.** Further analysis of requirements. Using the requirements contained herein as a baseline, the Working Group plans to convene a focus group of senior professionals with extensive recent experience in overseas posts, to further define the requirements

for knowledge systems to support posts. The results of this analysis will drive the design of a prototype knowledge system to serve as a test bed.

**2.** Development of comprehensive project plans. Structured project plans must be developed to support both the development and deployment of the prototype knowledge system as well as the development and deployment of two pilot knowledge systems at posts. These plans will include criteria for measuring the impact of these systems on business operations.

**3.** Involvement of the designated pilot posts. The two posts designated as pilot sites will become involved as soon as possible in the process.

Knowledge Management High Level Requirements Definition

The Knowledge Management Working Group was chartered to address recommendation 4.6 of the Overseas Presence Advisory Panel (OPAP) report. In summary, the OPAP report recommends that the foreign affairs agencies view the management of knowledge as a key function, and develop systems to allow development and sharing of knowledge resources.

Knowledge Management - Targets of Opportunity

The Knowledge Management Working Group met on four occasions during March 2000, and, as of March 30, has established the following list of Targets of Opportunity for implementing knowledge management at posts (i.e., identification of business requirements at a very high level). Note the list is in a priority order as determined by the working group.

**1.** Ability to communicate electronically among organizations at post, sharing email, files, notices, correspondence and other work products.
**2.** Wider availability of issue-specific databases at post. Examples are: INS Country Team Database, USAID Research Data (CDIE), Worldwide Refugee Database, Trade Issue Search Engine, Economic and Social Data, Enforcement-related Data
**3.** Greater use of workflow applications to allow employees to increase productivity. Examples are: travel processing, country clearance processing, procurement requests.
**4.** Wider access to ICASS information.
**5.** Development of a skills and expertise database for the foreign affairs community to allow identification of potential consultants by issue or skill area.
**6.** Easier access to sources of information in Washington, both within and outside headquarters organizations.
**7.** Universal access to the MPP process.
**8.** Support for crisis coordination (evacuations, alerts, health and safety)
**9.** Availability of expanded information about the post and the host country.
**10.** Expansion of the enforcement information available to that community at post.
**11.** (The above items were prioritized by the working group; items below were not

**12.** prioritized.)
**13.** Human Resources-related sources of information in areas such as payroll, classification, compensation plans and statistics.
**14.** Post calendaring and scheduling.
**15.** Availability of discussion areas, chat rooms, virtual meeting spaces and other electronic means of connecting people in real time. Discussions could be grouped by issue area or cluster.
**16.** Support for resource sharing at post (re-utilization of assets, group purchasing).
**17.** Take advantage of common communication facilities already established between INS and The Department of State.
**18.** Make cables available electronically, in a manner that allows searching.
**19.** Provide contracting support (information on sources of supply, procurement guidance)
**20.** Capture information related to post medical units and medical resources.
**21.** Housing information including available housing, lease information, information on local areas, forms, procedures for handling moves and other housing-related issues.
**22.** Local transportation information including motorpool information.

Knowledge Management - Challenges

The Knowledge Management Working Group also identified the following challenges which must be taken into account as we work toward a more knowledge-centered organization:

**1.** Low levels of staffing and turnover at post, plus difficulty in acquiring network support, create an imperative that knowledge management solutions be simple to administer.
**2.** Stovepipe systems: Incompatibilities create difficulty in making information more widely available.
**3.** There are infrastructure limitations between organizations at post. There are multiple network operating systems between the agencies, and converting to a common operating system would be prohibitively expensive. Agency Intranets are available only within the sponsoring agency
**4.** Lack of funding to support expanded capability. In addition, agencies hesitate to incur additional costs for systems support.
**5.** Lack of access to unclassified information residing on classified systems.
**6.** Limited telecommunications bandwidth is a concern in many parts of the world. Bandwidth limitations may limit the types of knowledge applications that can be used.
**7.** Incompatibilities exist regarding security requirements between agencies; particularly an issue for the more "public-oriented" agencies at post. Classification standards vary between agencies.
**8.** Developing and maintaining a willingness to share information between organizations.
**9.** Use of cables as the only official form of communication is limiting in a knowledge environment.

OPAP - Interagency Cooperation and Other Issues

While securing the active cooperation of the approximately 40 agencies operating overseas is a major challenge, we have to date received excellent cooperation. Clearly, the most important way to obtain agency cooperation is to develop IT systems and tools that they value, and we are making good progress in that direction. We are working to ensure interagency participation in the decision-making process and in promoting the value of the OPAP approach.

The Department of State is experienced in coordinating overseas interagency efforts and in managing large, globally implemented projects. We have been leveraging that experience to the OPAP initiative. We are also finding that our own recent IT successes have increased our credibility with the other agencies and this will go a long way to achieving cooperation. We have received broad recognition for our success with several very complex projects, especially the successful worldwide deployment of the ALMA global infrastructure. We had remarkable success in our Year 2000 initiative, going from a grade of F to an A in a very short time, and have put in place a sound IT governance process. This gives other agencies confidence that working with The Department of State can yield effective IT solutions.

The Interagency subcommittees have been working collaboratively to define requirements for a pilot OPAP Collaboration Zone and for the Knowledge Management System. We are conducting a comprehensive survey of all agencies to capture functional and technical requirements for the infrastructure. The Knowledge Management Working Group will be hosting a facilitated workshop to develop more detailed business requirements for the Knowledge Management System. We have enlisted agency representatives to work together with in leading our efforts, thus giving ownership to the entire group, not just to the Department of State as the lead agency.

We learned early on in the OPAP process that flexibility is vital. We must offer agencies different options for connectivity to the OPAP network and a flexible array of functional capabilities that meet agency needs. In collaboration with all foreign affairs agencies we are working to understand and accommodate individual agency functional and business requirements as well as technical constraints. We are also working to design solutions that have no negative impact on existing systems, and that enable agencies to leverage assets already in place, thus reducing overall costs and the need to change.

The OPAP Technology Working Group is designing a pilot architecture that minimizes risk and focuses on best value for all agencies. I am working to leverage my very active involvement as a member of the CIO Executive Council, using established relationships with other agency CIOs to help promote the OPAP initiative and enlist cooperation and enthusiasm. This fits well with the Council's focus on improving interagency efforts.

The friendships and working relationships of CIOs that have been built through the Federal Agency CIO Council are evident at the meetings of the Interagency Technology Subcommittee which I chair. It is clear all agencies agree that providing a modern

accessible and interoperable infrastructure to ensure that all employees of U.S. government agencies working overseas can communicate and collaborate with each other efficiently is a worthy goal.

While I am pleased with the level of interagency cooperation and participation displayed to date in developing solutions to the OPAP report IT-centered recommendations, I am concerned that we may not achieve full participation during the pilot program due to resource constraints. The President's FY 2001 budget includes $17 million in support of the recommendations for a common information technology platform overseas and a knowledge management system. If appropriated by the Congress, the Department of State will fund the design, development and pilot program deployment for all agencies represented at the pilot sites.

As the OPAP report noted, the technology to put in place the OPAP report recommendations is available. However, each agency has its own unique procedures and regulations governing the information placed on the systems, process for changing configuration of systems, and administering systems. Interagency agreement on security processes and procedures concerning risk mitigation and minimizing of system vulnerabilities are being addressed in the early phases of the project. Implementation and operation of shared IT infrastructure and systems may also require a change in the nature of IT current operations.

OPAP Conclusion

OPAP presents a challenge and an opportunity to succeed. The Department of State has the talent and the management skills to lead the interagency efforts to conclusion. We were successful in conquering the Y2K bug due to our management and technical expertise combined with Congressional support provided us. We also completed the worldwide deployment and implementation of ALMA at all of our overseas posts. These two examples were large complex projects very similar to potential worldwide application of OPAP solutions. Given continued support and the cooperation of the other agencies, the foreign affairs community will be successful in implementing the OPAP recommendations.

Information Technology is just one concern highlighted by the OPAP report, but IT can enable the Foreign Affairs Community to redesign America's overseas presence. I have witnessed the willingness of my CIO colleges in the Interagency Technology Subcommittee to work together to remove the technical barriers impeding interagency communication and collaboration and move toward an e-diplomacy business model.

## CAPITAL PLANNING AND MODERNIZATION

We are taking steps to ensure compliance with the Chief Financial Officers Act of 1990. The Chief Financial Officers Act of 1990, also known as Public Law 101-576, contains principle provisions to establish:

- CFO organizations in OMB and each agency;
- Improved accounting, reporting, and auditing practices;
- Improved financial systems;
- Improved asset management policies

The CFO Act of 1990 also mandates a government-wide Chief Financial Officer's (CFO) Council, and requires agencies to produce an annual progress report which is used by OMB to produce a government-wide financial management status report.

We are taking steps to ensure compliance with the requirements of Clinger-Cohen and OMB's A-11 guidance. This process was developed jointly by the Chief Information Officer, the Chief Financial Officer, and other senior management. In 1999, the Department inaugurated a new IT Capital Investment process that allocates all Central Fund resources. This process is chaired by the Under Secretary for Management to:

- Meet requirements of Clinger-Cohen and OMB A-11; and

- Establish and Maintain effective working relationships with key stakeholders, giving them active roles in IT capital planning and investment.

### The Information Technology Program Board (ITPB)

Under this arrangement the senior management group, the Information Technology Program Board (ITPB), advises the Under Secretary for Management on funding allocations for the Department's IT activities. The CIO is the second chair of the ITPB and members of the ITPB are at the Assistant Secretary level representing the Department's regional, functional, and management bureaus.

### The ITPB Charter

The Information Technology Program Board (ITPB), an advisory entity to the Under Secretary for Management, is the highest-level body that addresses Information Technology (IT) issues in the Department of State (DoS). The ITPB has two primary purposes: to assess and determine needs for IT resources to support DoS strategic missions, and to ensure that IT resources available to DoS are used effectively and efficiently in support of those strategic missions.

Functions

Specific functions of the ITPB are to:

- Approve and issue DoS IT Strategic and Performance Measurement Plans, ensuring that they are fully supportive of the DoS Strategic Plan.

- Approve DoS budget requests for IT resources, ensuring that initiatives being undertaken are consistent with the current IT Strategic and Performance Measurement Plan.

- Allocate available IT resources on the basis of sound management and investment practices, and in particular, such factors as furtherance of DoS missions, favorable returns on investments, and the ability of IT project groups to make effective use of resources.

- Approve and issue DoS capital management procedures for initiating IT projects, implementing IT systems, and evaluating the cost and effectiveness of those systems over their entire life-cycles.

Membership

The Under Secretary for Management serves as the Chair of the ITPB. The Department's Chief Information Officer (CIO) serves as the Deputy Chair. Members of the Board include:

Executive Secretary of the Department
Assistant Secretary for Consular Affairs
Assistant Secretary for Administration
Assistant Secretary for Diplomatic Security
Assistant Secretary for one Regional Bureau (rotated periodically)
Assistant Secretary for one Functional Bureau (rotated periodically)
Chief Financial Officer (CFO)

Staff Support

The ITPB has no full-time staff. It is supported by staff members of FMP, IRM, and A as needed.

The ITPB depends heavily on two lower-level IT groups, the Management Review Advisory Group (MRAG) and the Technical Review Advisory Group (TRAG), for preliminary evaluations of IT issues, projects, and budget matters. The MRAG and TRAG continually evaluate IT projects, systems, and resources and provide the ITPB

with joint recommendations regarding those projects, systems, and resources, along with proposed solutions to enterprise-wide IT problems.

## Meetings

The ITPB meets several times each year to support the Department's regular budget and capital planning cycles. These and other ITPB meetings, as required, will be called by the Under Secretary for Management.

## ITPB Standard Operating Procedures

Scheduling Meetings – In general, the time and place of ITPB meetings will be announced at least a week in advance. Meeting announcements will be accompanied by planned agendas and background documentation pertinent to the subjects to be considered.

Attendance at Meetings – Members of the ITPB are expected to participate in each meeting or, if that is not possible, to send the person officially acting in that position. Depending on the size of the meeting room, members or designated representatives may bring other persons to ITPB meetings, if necessary; however, those persons may not participate in the ITPB discussion unless specifically asked to do so by a member of the ITPB.

Meeting Chair – The Under Secretary for Management will chair ITPB meetings. In absence of the Under Secretary, the Chief Information Officer (CIO) will chair the meetings.

Information/Presentations – To conserve the time of the ITPB, most of the information presented to it will have been pre-evaluated by the Management Review Advisory Group (MRAG) and the Technical Review Advisory Group (TRAG). In addition, most of the presentations to the ITPB will be made by members of the MRAG or TRAG. However, managers of major IT projects or other IT projects of special significance or interest may be called upon to provide direct input to the ITPB. Also, at the discretion of the Under Secretary for Management, bureau sponsors may be permitted to make presentations about their proposed projects to the ITPB.

Recommendations – The ITPB is an advisory function for the Under Secretary for Management. It provides a broad representation of Departmental interests and a variety of viewpoints helpful in decision-making. ITPB recommendations will be presented to the Chair in the form of decision memoranda.

Documentation – The staff of FMP and IRM will have responsibility for documenting decisions made by the ITPB and for distributing this documentation to members of the ITPB. The ITPB structure is shown as follows in Figure 2.

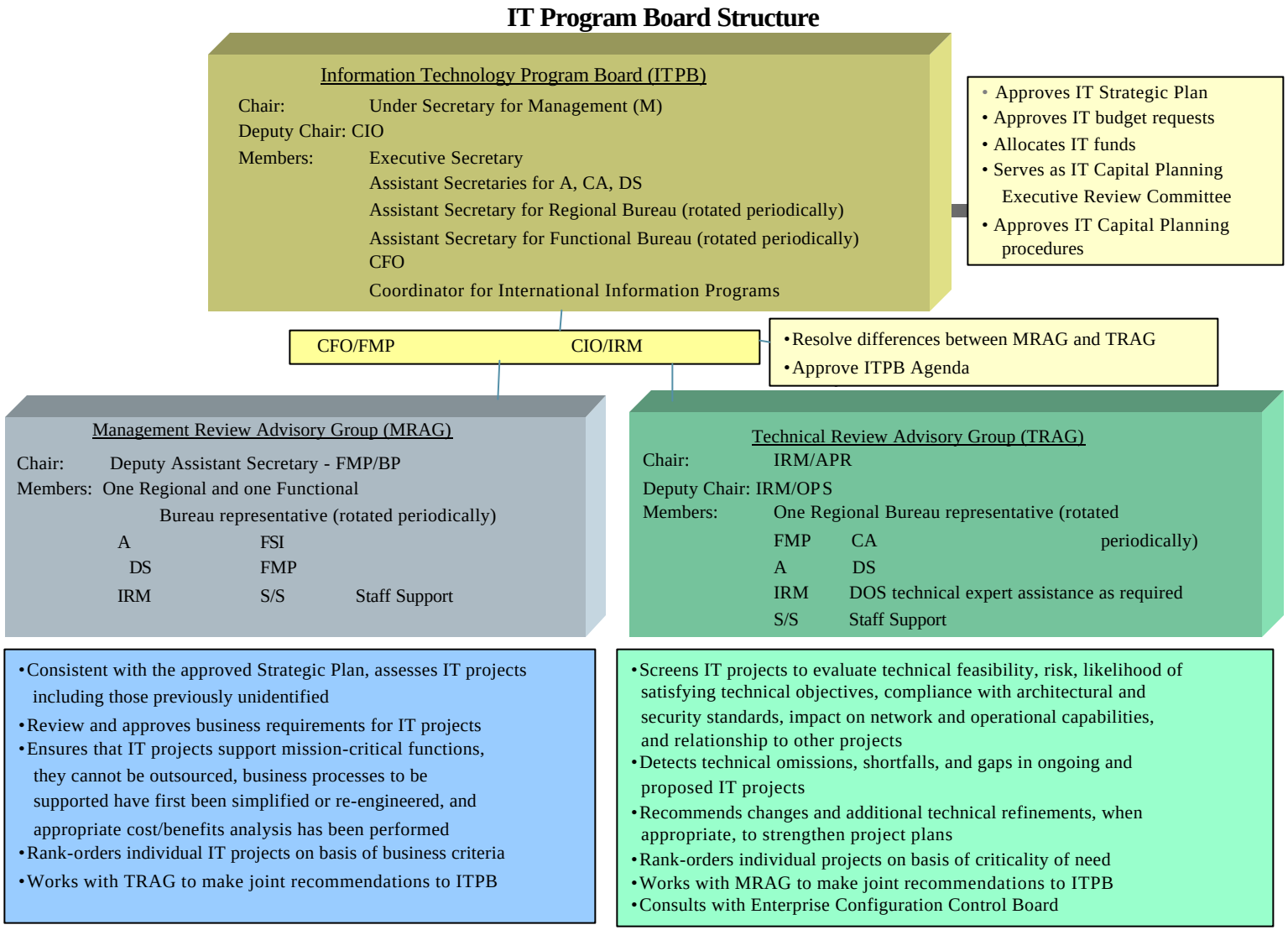


**Figure 6. Information Technology Program Board (ITPB) Structure**

The ITPB is supported by two advisory groups: 1) the Management Review Advisory Group (MRAG) that evaluates the investment potential of IT projects and their ability to support the Department's IT Strategic Plan; and 2) the Technical Review Advisory Group (TRAG) that assesses the technical merits of IT projects and their potential impact on the infrastructure.

Together, the ITPB, MRAG, and TRAG ensure that IT projects and systems:

- Support the mission of the Department of State;
- Represent sound investments;
- Are carried out in the most cost-effective manner possible; and
- Present managed technical risk.

Specific formats for project plans have been defined that tie to our established project management methodology – Managing State Projects – a methodology modeled after a successful approach used by the CIA. Project plans include such sections as:

- Return On Investment;
- Benefit Cost Analysis (for all major projects);
- Security Plan;
- Alternatives Analysis;
- Outcome and Output Performance Measures;
- Two year cost estimates with associated Milestones; and
- A five-year life cycle cost estimate.

A subset of this information is published in our well established IT Tactical Plan.

These project plans are provided to MRAG and TRAG members and to an IT Configuration Control Board that determines the impact on the infrastructure. In addition, change requests made to the CCB can initiate action to the ITPB if the change(s) requested are determined to have a significant impact on the architecture or infrastructure, or will require significant resources to implement or maintain.

These entities review projects against the Department's Strategic Plan, the IT Strategic Plan, and the Information Technology Architecture (ITA). The ITA was published in April of 1999, and provides a framework for mapping business requirements to technical solutions and provides a framework for specifying IT architectural components and standards. The framework of the ITA was based on guidance published by the CIO Council in late 1998. We are continually enhancing the ITA to ensure that it remains current with our plans and advances in technology.

Based on the project plans and decisions taken by the ITPB, the IT Tactical Plan presents the estimated funding requirements. However, we recently published our new IT Strategic Plan in January 2000, and are currently working to refine our cost estimates based on our updated Goals and Objectives.

The Department has a robust IT Planning and Management process currently in place. We have a series of key IT planning documents including our new IT Strategic Plan, IT Tactical Plan, and Information Technology Architecture that link to, and are driven by, the International Affairs Strategic Plan and the Department Strategic Plan. These planning documents guide and drive all of our IT work and processes. We have repeatedly been asked for copies of these plans by other government agencies including the Executive Office of the President.

State Department IT Strategic Planning

Our IT Strategic planning has been highly praised, and our Five Year Goals paper and recent IT Strategic Plan have been highlighted in the trade press. The National Research Council Office of International Affairs published a study titled The Pervasive Role of Science, Technology, and Health in Foreign Policy: (1999) Chapter 3, p.45, Broadening and Deepening Science, Technology, and Health Competence within the Department of State. This article praised our five-year plan and made mention of the plan's early achievements. This article also made the following recommendation: "The Secretary, the Administration, and Congress should ensure that the Department's five-year information technology modernization plan stays on course and is fully funded for its successful implementation and also for necessary ongoing maintenance and upgrades."

Additional management items were raised in a separate GAO modernization report Department of State IRM Modernization Program at Risk Absent Full Implementation of Key Best Practices, GAO/NSIAD-98-242, September 1998. These have also been resolved. With the Undersecretary for Management Cohen's support, IRM took the following steps to address the issues presented in the GAO report:

1. Working closely with the Chief Financial Officer and other senior management, we are taking steps to implement an enhanced Capital Planning Process to involve all the key stakeholders and meet the requirements of Clinger Cohen and OMB's A-11.
2. Implemented a working Configuration Control Board and are currently expanding the role of this CCB, further strengthening the interrelationship with the Capital Planning Process.
3. Published an Enterprise IT Architecture that is modeled after guidance issued by the Federal CIO Council.
4. Included output and outcome measures in our IT Tactical Plan and tie outcomes to mission effectiveness or efficiency.
5. Instituted a disciplined life cycle management process – called Managing State Projects – to help ensure a consistent approach to all aspects of project management.
6. Focused on a few well-articulated goals that are presented in our new IT Strategic Plan published in January of this year.

The CIO is actively engaged in ensuring the success of our IT Modernization projects:

- Works closely with the CFO and other senior management to develop effective budget plans, accompanying excellent technical plans, that have succeeded in greatly increasing our IT modernization budget.

- Engages peers at the Assistant Secretary level by meeting with them regularly.

- Conducts regular conferences with our overseas Information Management Officers (IMOs) to share vision, goals and current activities.

The success of these improvements in our planning processes is best exemplified in recent key projects:

1. The Department of State successfully deployed a fully modern IT infrastructure to the desktop of every employee at 233 overseas posts, providing robust office automation tools and e-mail access to the Internet. This modernized infrastructure provides the foundation for enhanced, information age communication and collaboration for U.S. diplomats.

2. As a result of the Department of State's proactive efforts to ensure that all of its IT systems would be Y2K compliant, little or no anomalies in our systems were encountered during the rollover. The Chairman of the House Subcommittee on Government Management, Information and Technologies, Congressman Stephen Horn, issued a report card raising our "F" in 1998 to an "A" in 1999. In recognition of this progress, The Department of State was also awarded a Government Computer News award for excellence in technology.

3. To ensure uninterruptible international emergency voice communications and to improve local communications, we fielded 883 satellite telephones, 106 emergency and evacuation, or "E&E" net radio systems, and some 5040 hand-held radios at overseas posts.

4. We now have a single modern e-mail package, MS Exchange, linking all Department offices and overseas posts

While we have made such significant progress modernizing our IT, we still have a lot of work ahead of us. We must

- Continue to deploy major improvements to our administrative and management systems such as GEMS personnel and our financial systems

- Continue to deploy CableXpress - a popular and effective new front end to our formal message traffic system

- We must replace our existing vintage World War II messaging system with a new system that provides a more robust and scaleable network taking advantage of today's technology.

- Continue to refresh our overseas unclassified infrastructure and modernized our overseas classified IT infrastructure. There are many unexploited security techniques and technologies that we must take advantage of to effectively secure the Department's worldwide IT and physical resources. We will create a state-of-the-art, cost-effective global network that maximizes access to worldwide information. This network will provide features like more robust world-wide secure communication, transmission of secure email and classified documents, and connectivity to DoD's classified network (SIPRNET).

- Implement the five Goals of the new IT Strategic Plan. This will require resources to address the gaps in our IT infrastructure. Our new IT Strategic Plan focuses on building a robust world-wide network, expanding the tools available to our substantive officers, revamping our obsolete messaging systems, centralization and streamlining our administrative systems, and enhancing the skills and retaining our core IT workers.

My new IT Strategic Plan presents this vision and lays out the road ahead of us for the next five years. The current focus of the OPAP pilots is on the unclassified infrastructure – an area in which we are fully modernized. The Department of State will require sustained funding in order to achieve the goals in the ITSP. Cornerstones to achieving these goals are the modernization of the classified infrastructure and sustained technology refresh of the entire enterprise – both will also be required in order to pursue the OPAP objectives into the classified arena in the future.

## CONCLUSION OF TESTIMONY

The information technology requirements associated with modern diplomacy will likely increase over the next few years. Two recent studies, both conducted by prominent diplomatic experts, discuss the radical changes expected to occur in the conduct of diplomacy and international affairs[2]. As we addressed in this report, the more recent report of the Overseas Presence Advisory Panel (OPAP) demands a leadership role from The Department of State in ensuring interagency exchange of information and robust interoperability. Collectively, the changes that can be foreseen will subsequently generate a demand for far greater connectivity with other countries, Non-Government Organizatioins (NGOs), and various publics. As discussed in this report, security requirements, challenges, and demands are already increasing and will continue to do so. Likewise, there will be increased demand for information access, intelligent analytical tools, powerful search engines, and collaborative processing - within The Department of State, with other organizations, and with other technologies. The Department is committed to supporting our diplomats and the foreign affairs agencies as we move into

[2] Stimson and CSIS reports

this new information age. We are seeking to establish a robust IT environment that will support what we have termed *e-Diplomacy*, the conduct of diplomacy in the age of the Internet and other technological advances. We must continue to make the investments needed to support this vision and add value to the conduct of international affairs.

Although we have made great strides in the past two years, the Department faces significant IT challenges it has only most recently begun to address. Chief among these is providing a robust, secure global network that gives our domestic and overseas staff desktop access to the classified, sensitive but unclassified (SBU), and unclassified information required for the job. In the increasingly interconnected world in which they operate, our diplomats and other officers are severely short-changed by the technological limitations they face today. We must provide global connectivity and full Internet access at all locations. We must address the knowledge needs of diplomats in new and creative ways, giving them easy access to multiple, timely sources of information at their fingertips, facilitating sharing of best practices, and fostering collaboration across the foreign affairs community. To this end, we have published an IT Strategic Plan for FY2001-FY2005. The plan sets the direction and five goals for IT support for the Department's international affairs mission in the early years of the new millennium. The Department has adopted these goals at the highest levels. This IT direction closely parallels the two recent outside reports cited above, documenting the need for radical changes in diplomacy and associated supporting infrastructure. As previously noted, another study produced by the National Research Council (NRC)[3] highly praised our five year plan and calls for significant investment to implement The Department of State's IT Strategic Plan. This study recommends the following:

> The Secretary [of The Department of State], the Administration, and Congress should ensure that the Department's five-year information technology modernization plan stays on course and is fully funded….

To address these challenges and build the global network we need, we must address an array of security concerns, some of which are unique to the Department's role as the lead foreign affairs agency. Our systems have been repeatedly targeted by internal and external threats having ever-increasing levels of sophistication. Our overseas posts are heavily dependent on a local foreign nationals workforce. As communications capabilities increase, so do the security threats and risks associated with unauthorized access to sensitive information. As we connect our networks to the Internet, we must be sure to protect the integrity of our information assets. Accordingly, we have embarked on several ambitious and vital initiatives to devise and implement cost-effective security solutions that will enable us to manage and minimize risk, while providing our professionals with the information tools they need. In short, we are committed to deploying a viable security infrastructure that meets our business and security requirements.

---

[3] *The Pervasive Role of Science, Technology, and Health in Foreign Policy, Imperatives for the Department of State*, National Research Council, 1999.

The conduct of international affairs is highly information-intensive. To protect our vital national interests, The Department of State must have access to current and accurate information and the ability to disseminate and share that information among the international affairs community. This demands *e-Diplomacy* and the most effective information management tools, systems, and networks possible. The nation runs a grave risk if we fail to provide our overseas staff with ready access to the information they need to make informed decisions and provide the excellent analyses and advice the Department's stakeholders depend on. Accordingly, we must finish the job of modernization and position the nation for *e-Diplomacy*. We must continue to make the investments needed to support this vision and add value to the conduct of international affairs.